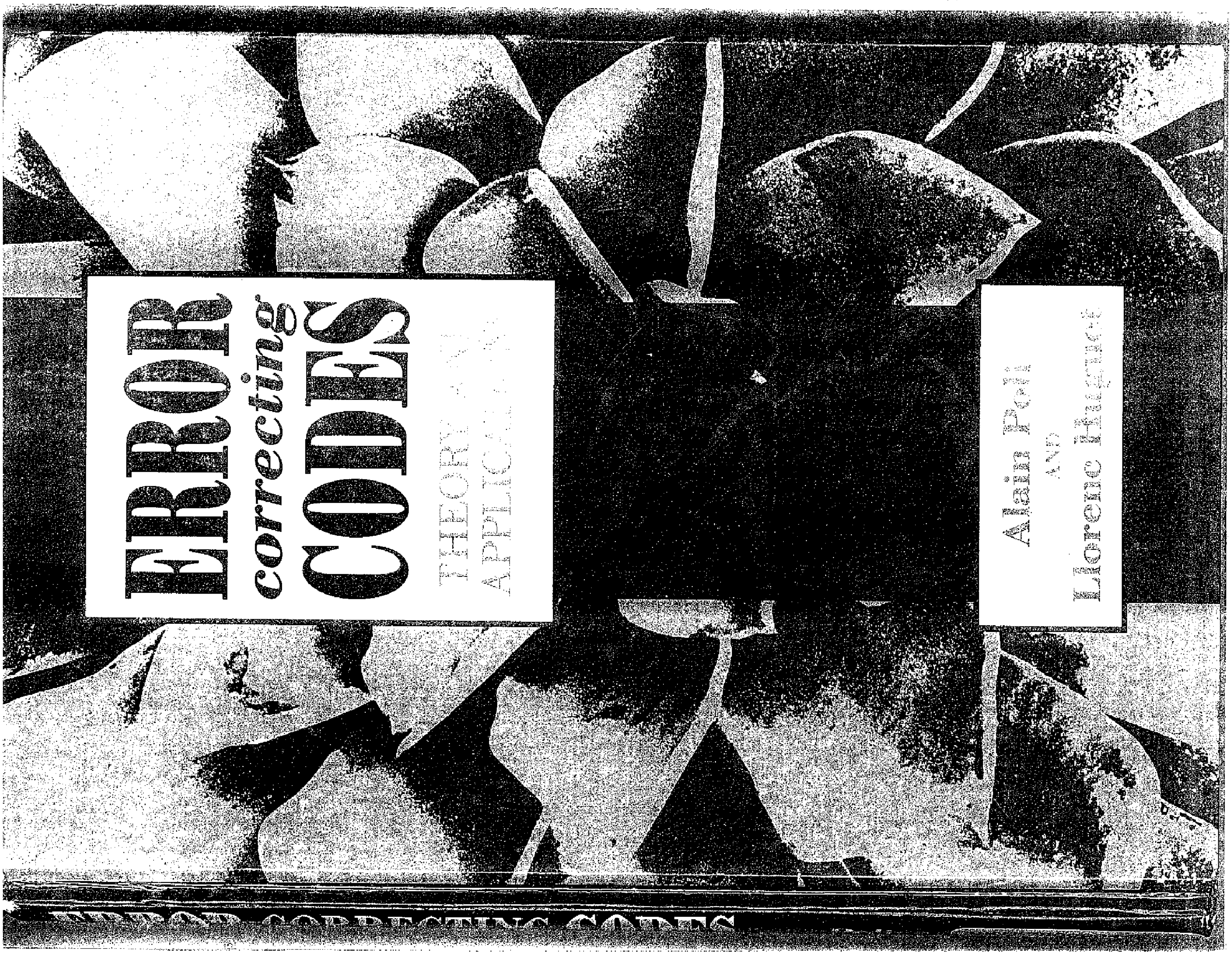
Exhibit P


ERROR
correcting
CODES
Alain Poli
AND
Llorenç Huguet

Error Correcting Codes

Theory and Applications

ALAIN POLI
AND
LLORENÇ HUGUET

TRANSLATED BY
IAIN CRAIG
University of Warwick

PRENTICE HALL
MASSON

First published 1992 by
Prentice Hall International (UK) Ltd
Campus 400, Maylands Avenue
Hemel Hempstead
Hertfordshire, HP2 7EZ
A division of
Simon & Schuster International Group

This book was originally published under
the title *Codes Correcteurs*
by Alain Poli and Llorenç Huguet

Printed and bound in Great Britain by
Hartnolls Ltd, Bodmin

Library of Congress Cataloging-in-Publication Data

Poli, Alain, 1939–
[Codes correcteurs. English]
Error correcting codes / Alain Poli and Llorenç Huguet.
p. cm.
Translation of: Codes correcteurs.
Includes bibliographical references and index.
ISBN 0-13-284894-5: $80.00
1. Error correcting codes (Information theory)
I. Huguet, L. (Llorenç), 1953– . II. Title.
QA268.P6613 1992
005.72—dc20 92-12129
CIP

British Library Cataloguing in Publication Data

A catalogue record for this book is available
from the British Library

ISBN 0-13-284894-5 (hbk)

1 2 3 4 5 96 95 94 93 92

CHAPTER FOUR

Classical Error Correcting Codes

The transmission of information over a communication system risks introducing errors into the sequence of transmitted symbols. The output of the transmission channel can be different from the input. In the binary case this is revealed by changes from 0 to 1 or vice-versa. To combat the noise in the channel, we use blocks of n symbols to transmit k symbols of information.

Such a block with a length of n is called a *codeword*.

4.1 Introduction

The communication system that we are considering is shown in Figure 4.1.

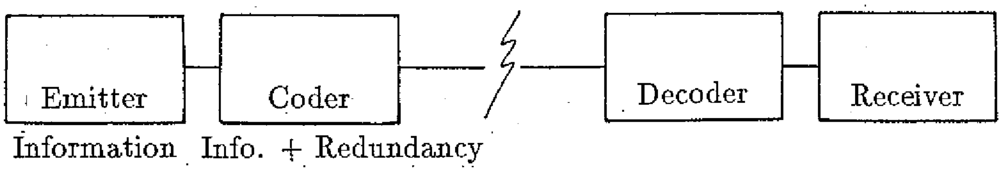


Figure 4.1

To perform transmission error detection and correction, it is necessary to add symbols, called *control symbols* (or *parity check*), to the symbols corresponding to the information that is to be transmitted. This addition is performed according to a rule C (called the *coding rule*) which is known to the transmitter and to the receiver. Thus, the decoder verifies that the sequence that it has just received satisfies the rule C or not. If it does not satisfy the rule, it is certain that at least one error has occurred. The decoder then will try to correct the sequence.

This rule C, which characterizes the code being used, can be considered as a bijective function between the set of information sequences of length k and the sequences of length n which are the codewords to be transmitted over the channel. The encoding and decoding operations must be easily implemented in the transmitter and receiver, respectively. This means that the rule C must have a simple structure in the form of a mathematical expression.

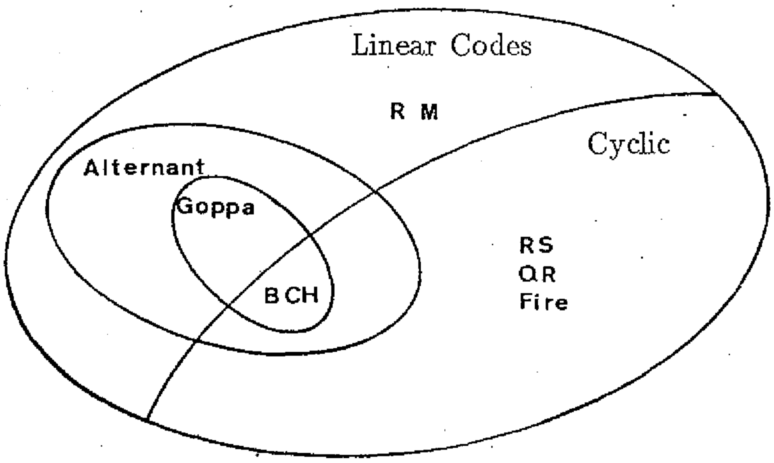


Figure 4.2

This is the case for the codes that we are going to examine in this chapter: error detecting and error correcting codes (see Figure 4.2).

In this chapter, we are going to consider block codes, in particular, linear codes. We will undertake the study for binary codes, but it can easily be generalized to codes formed over any finite field $GF(q)$, where q is a power of a prime number p.

A binary block code $\mathcal{C}$ is a set of sequences of 0 and 1, each of which have the same length. Each sequence is called a codeword. The parameters of such a code are:

- Length of codeword: n.
- Cardinality of the code: N.
- Transmission rate: $R = (\log_2 N)/n$.
- minimum distance: d.

DEFINITION 1. The (Hamming) distance between two sequences of length n is equal to the number of positions in which they differ.

The minimum distance d of the code is the least Hamming distance between two distinct codewords. This parameter indicates the detection and correction capacities of the code. As far as error correction is concerned, it is necessary, not only to detect errors, but also to localize them in the sequence received from the output of the transmission channel, and then to reconstruct the codeword which has been transmitted. In this sense, decoding can be considered as a function from the set of all n-tuples into the set of all codewords.

4.2 Linear Codes

As we said in the introduction, we are going to consider the finite field $GF(2)$ in this section (cf. Chapter 3). But all the results are easily generalizable to the case of any finite field $GF(q)$.

Let $V = [GF(2)]^n = \{v = (v_1, v_2, \ldots, v_n) \mid v_i \in GF(2)\}$ be the vector space of dimension n over $GF(2)$ (cf. Section 2.2.2).

4.2.1 Definitions and basic properties

A binary code $\mathcal{C}$ is a subspace of V. It is said to be linear if it has the structure of a vector subspace.

If the dimension of this subspace is k, then the linear code $\mathcal{C}$ has 2^k codewword. It is written $\mathcal{C}(n, k)$, where the parameters k and n are called the *dimension* and *length* of the code, respectively.

DEFINITION 2. Given a vector $v = (v_1, \ldots, v_n) \in V$, we define the weight of v, written $w(v)$, as the number of its non-zero coordinates.

REMARK 1. The Hamming distance $d(u, v)$ is equal to $w(u - v)$. The minimum distance of a linear code (written d) is therefore equal to its minimum non-zero weight.

The parameter d is fundamental as far as the power of correction/detection of the code is concerned, as we will see in Lemma 1.

DEFINITION 3. Decoding with the minimum distance rule makes each input vector corresponding to the codeword that is closest to it.

It is therefore possible to correct up to $\lfloor (d-1)/2 \rfloor$ errors per codeword.

Lemma 1. *A linear code with minimum distance d can detect up to $d - 1$ errors and correct up to t, with $d = 2t + 1$ or $d = 2t + 2$, if the minimum distance decoding rule is used.*

PROOF. Assume that we have transmitted the codeword u of C and we receive the vector $v = u + e$ in V, e being the error vector. The non-zero components of this vector represent the transmission errors. We have:

$$w = w(e) = w(v - u) = d(u, v)$$

If $w < d$ then e is not a codeword, and the error has been detected.

If $w \geq d$ then it could be that e is a codeword, and therefore the received vector will also be a codeword since C is a subspace. The error cannot therefore be detected.

Let us consider the spheres of radius t centered on the codewords. By definition of d they are disjoint (see Figure 4.3).

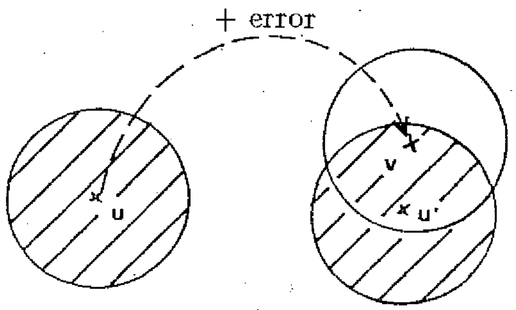


Figure 4.3

As far as correction is concerned, we note the following by the minimum distance decoding rule:

- If the vector that has been receieved, v, is in the sphere centered on the codeword u, then we can decode v by u. Then:
- If we have at least t transmission errors, then we are sure that we can correct these errors.
- If there are more than t errors, then v can be in another sphere whose center is a codeword different from the one that has been sent. In this case, decoding will give a poor result.

□

DEFINITION 4.

(1) A linear code $\mathcal{C}$ with length n, dimension k and minimum distance d, is often written $\mathcal{C}(n,k,d)$.

(2) A code which corrects up to t errors is often called a t-correcting code.

4.2.2 Generator matrix, control matrix

We take $\{g_1, g_2, \ldots, g_k\}$ as the basis of the linear code $\mathcal{C}$. We can then write:

$$\mathcal{C} = \{u \in V \mid u = a.G, a = (a_1, a_2, \ldots, a_k) \in [GF(2)]^k\}$$

where G is the $k \times n$ matrix whose rows are the g_i in the basis of $\mathcal{C}$. This matrix G is a generator matrix of $\mathcal{C}$.

Let us consider the vector subspace orthogonal to $\mathcal{C}$:

$$\mathcal{C}^\perp = \{v \in V \mid < u, v >= 0 \text{ for all } u \in C\}$$

(cf. Section 2.2.2).

The dimension of $\mathcal{C}^\perp$ is $n-k$ (cf. Chapter 2, Proposition 43), and it can be considered as the linear code $\mathcal{C}^\perp(n, n-k)$ which has one $(n-k) \times n$ generator matrix (which is written as H). It is clear that, by these definitions, we can set:

$$\mathcal{C} = \{u \in V \mid u.H^t = 0\}$$

This matrix H is called the *parity-check matrix* (or *control matrix*) of $\mathcal{C}$.

REMARK 2. We can also consider a linear code $\mathcal{C}$ as the image of a linear function from $[GF(2)]^k$ into $[GF(2)]^n$, which has G as its matrix.

In the same way, C can be defined as being the kernel of a linear function from $[GF(2)]^n$ into $[GF(2)]^{n-k}$ whose matrix is H.

EXAMPLE 1. If we want to construct a linear code $C(6,3)$, it is necessary to choose three linearly independent vectors in $[GF(2)]^6$, which give a basis for C. Let, for example:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

We will have:

a	$C = \{v = aG\}$	$w(v)$
000	000000	0
001	110110	4
010	011101	4
011	101011	4
100	100101	3
101	010011	3
110	111000	3
111	001110	3

We could detect up to 2 errors and correct 1, because the minimum weight of this code is 3.

To construct the control matrix H, it is necessary to give a basis of solutions to the system of linear equations that follows:

$$(v_1, v_2, v_3, v_4, v_5, v_6).H^t = (0,0,0)$$

that is, it is necessary to construct a basis for the kernel of H. We must have (using rows of G):

$$v_1 + v_4 + v_6 = 0$$

$$v_2 + v_3 + v_4 + v_6 = 0$$

$$v_1 + v_2 + v_4 + v_5 = 0$$

By choosing, for example, the free variables v_3, v_4 and v_6, we have:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

The orthogonal code $C^{\perp}$ is therefore the linear code with parameters $n = 6$ and $k = 3$ that we show below (with $a \in [GF(2)]^3$):

a	$C^{\perp} = \{u = aH\}$	$w(u)$
000	000000	0
001	011010	3
010	110110	4
011	101100	3
100	110001	3
101	101011	4
110	000111	3
111	011101	4

REMARK 3. Another choice of free variables would give us another basis for solutions to the same system, and, therefore, another parity-check matrix for the code $C(6,3)$. In other words, there are several bases for a vector subspace.

The parity-check matrix of a linear code can be used in the detection and the correction of errors, as we will see below (cf. Section 4.2.6). Furthermore, it gives us a lower limit for the minimum weight of the code, as we will now see.

Proposition 1. *Let C be a linear code which has parity-check matrix H. There exists one codeword with weight w if and only if there exist w columns in H which are linearly independent.*

PROOF. We know that a codeword v satisfies the matrix equation $v.H^t = 0$. If we write the i^{th} column of H as h^i (that is the i^{th} row of H^t), we can then write the preceding matrix equation as:

$$\sum_{i=0}^{n} v_i.h^i = 0$$

□

Corollary 1. *A linear code C with a parity-check matrix H has a minimum weight at least w if and only if every set of $w-1$ columns of H is a free family.*

PROOF. Immediate.
□

REMARK 4. The minimum distance d of a linear code $\mathcal{C}(n,k)$ must satisfy $d \leq n-k+1$ (proof as exercise).

4.2.3 Projective linear codes

A linear code $\mathcal{C}(n,k)$ is said to be *projective* if and only if the columns of its generator matrix G are pairwise independent (i.e., no column is a scalar multiple of any other). For the binary case, this means simply that all columns are pairwise distinct.

REMARK 5. The codes $\mathcal{C}$ and $\mathcal{C}^{\perp}$ with generator matrices G and H given in example 1 are examples of projective codes. By Corollary 1, the orthogonal code to a linear code which is at least 1-correcting is always projective.

4.2.4 Extended codes, truncated codes

Sometimes it is interesting to find new codes from existing ones in order to improve the parameters of the original code. This is the case for extended and truncated codes.

4.2.4.1 Extended codes

Let $\mathcal{C}(n,k,d)$ be a linear code. We consider the extended linear code $\hat{\mathcal{C}}(n+1,k)$ with minimum distance d or $d+1$, where each code word $\hat{v} = (v_1, v_2, \ldots, v_n, v_{n+1})$ is such that:

$$v = (v_1, v_2, \ldots, v_n) \in C$$

and $v_{n+1} = f(v)$ for some function f.

The more classical case is the following:

$$v_{n+1} = f(v) = -\sum_{i=1}^{n} v_i$$

All the codewords in $\hat{C}$ have even weight. We say that we have added a parity bit. The parity-check matrix $\hat{H}$ of $\hat{C}$ is obtained by adding a row of 1s and a column of 0s to the parity-check matrix H of $\mathcal{C}$ in the $n-k$ first positions and a 1 in the $n-k+1^{\text{th}}$ position.

EXAMPLE 2. The extended code for the code given in Example 1 is:

a	$\hat{C}$	$w(\hat{v})$
000	0000000	0
001	1101100	4
010	0111010	4
011	1010110	4
100	1001011	4
101	0100111	4
110	1110001	4
111	0011101	4

Its parity-check matrix is:

$$\hat{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

4.2.4.2 Shortened codes

Let $C(n,k,d)$ be a linear code. We infer a shortened linear code $C^*(n,k)$ by removing one or more of the coordinates from each codeword in $C(n,k,d)$. Each time that we remove a coordinate, the length reduces by one, while the dimension remains constant. The minimum distance can diminish by one, but often we can remove a coordinate which does not alter the minimum distance d. The generator matrix G^* of the shortened code is obtained from the generator matrix G of the original code by removing the column corresponding to the coordinate that has been eliminated from the code words.

EXAMPLE 3. The shortened code that is obtained from the code given in Example 1 by removing the second coordinate from codewords has as its generator matrix:

$$G^* = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

The codewords are:

a	$C^* = \{v = aG^*\}$	$w(v)$
000	00000	0
001	10110	3
010	01101	3
011	11011	4
100	10101	3
101	00011	2
110	11000	2
111	01110	3

4.2.5 Linear codes in systematic form

We have seen the importance of the generator matrix G and parity-check matrix H of a linear code $\mathcal{C}(n,k)$. The fact that we can obtain one from the other requires the solution of a system of $n-k$ linear equations in n unknowns (Gauss' method). It is therefore prudent to use those linear codes which make this as easy as possible. This is the case for codes in systematic form.

Definition 5. A linear code $\mathcal{C}(n,k)$ is said to be in systematic form when the information a in $[GF(2)]^k$ is in the prefixed coordinates of the corresponding codeword. (The problem is more complicated for multivariable codes, cf. Chapter 6.)

Without loss of generality, we can consider that these prefixed coordinates in each codeword are the first k positions. In this case, the generator matrix has the identity matrix in its first k columns (cf. Proposition 40, Chapter 2):

$$G = (I_k \,||\, P) \text{ where } P \text{ is a } k \times (n-k) \text{ matrix}$$

Remark 6. In the case of cyclic codes, we sometimes consider the identity over the k last columns (cf. Chapter 3).

Definition 6. Two linear codes $\mathcal{C}$ and $\mathcal{C}'$, with the same parameters n and k, are said to be equivalent if and only if there exists a permutation σ of the coordinates which transforms every codeword of $\mathcal{C}$ into a codeword of $\mathcal{C}'$. That is:

$$G' = G.\sigma \text{ and } H' = H.\sigma$$

G and G' are the generator matrices, and H and H' are the parity-check matrices of C and C', respectively.

Proposition 2. *Every linear code $C(n,k)$ is equivalent to a linear code in systematic form such that its generator and parity-check matrices are respectively:*

$$G' = (I_k \parallel P) \text{ and } H' = (-P^t \parallel I_{n-k})$$

Proof. By linear combination of the rows of G we can find the identity matrix of order k, because the rank of the matrix is k, and this does not change the vector subspace C (we have only changed the basis). By a permutation of columns (which will change the subspace C) we can place the identity matrix in the first k columns of G thus obtaining the generator matrix G' of a linear code in systematic form (in fact, it is Gauss' method that is used). Finally, the rows of H' are orthogonal to the rows of G'. As they are linearly independent, then H' can be considered to be the parity-check matrix of the linear code in systematic form.
□

Example 4. A code in systematic form which is equivalent to the linear code given in Example 1 can be obtained in the following way. First, we substitute the third row of G for the sum of the first and third, then we form the permutation (1 3 5 4 2 6) (see Example 2, Chapter 2). We obtain the generator matrix G' thus:

$$G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

and the parity-check matrix:

$$H' = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

4.2.6 Decoding linear codes

We are now going to present a minimum distance decoding rule using an array (a *standard array*) in which each input vector is decoded by the codeword which is in the same column of the array. After several results about the construction of this array, we will see that it is the parity-check matrix that is used to tell which is the codeword corresponding to the input vector: this is done via a calculation of the syndrome.

The algebraic results given here rest on those of Section 2.1.2.

DEFINITION 7.

(1) Let $\mathcal{C}(n,k)$ be a linear code, and let u be an element of $[GF(2)]^n$. We consider the class of u modulo $\mathcal{C}$: $u+\mathcal{C} = \{v' \in [GF(2)]^n \mid v' = u+v, v \in \mathcal{C}\}$. We will say that $u+\mathcal{C}$ is a coset of $\mathcal{C}$, where u is a representative (called the *coset-leader*).

(2) The standard array contains a different coset of $\mathcal{C}$ in each row.

The cardinality of each coset of the code is 2^k (cf. Corollary1, Chapter 2).

Proposition 3. *For a linear code $\mathcal{C}(n,k)$, there exist 2^{n-k} different cosets which form a partition of the vector space $[GF(2)]^n$.*

PROOF. cf. Corollary 1, Chapter 2. The standard array therefore has 2^{n-k} rows.
□

4.2.6.1 Construction of the standard array

We can write all the vectors in $[GF(2)]^n$ as the elements of an array with 2^k columns and 2^{n-k} rows. Each row is a coset of $\mathcal{C}$.

$$\begin{array}{ccccccccc}
\mathcal{C} & : & 0 & v_1 & v_2 & \cdots & v_j & \cdots & v_N \\
u_1+\mathcal{C} & : & u_1 & u_1+v_1 & u_1+v_2 & \cdots & u_1+v_j & \cdots & u_1+v_N \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
u_i+\mathcal{C} & : & u_i & u_i+v_1 & u_i+v_2 & \cdots & u_i+v_j & \cdots & u_i+v_N \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
u_M+\mathcal{C} & : & u_M & u_M+v_1 & u_M+v_2 & \cdots & u_M+v_j & \cdots & u_M+v_N
\end{array}$$

where $N = 2^k - 1$ and $M = 2^{n-k} - 1$.

This is the standard array for decoding.

We can use this array to give the following decoding rule. Let v' be the received vector. We decode v' by the codeword v which is in the same column as v' in the standard array.

REMARK 7. If we take the coset-leader as a minimum weight vector in each coset, then decoding using the standard array coincides with the minimum distance decoding rule.

Lemma 2. *If $C(n,k)$ is a linear t-correcting code, then all the vectors of weights less than or equal to t are in different cosets. In this case, we have the inequality:*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t} \leq 2^{n-k}$$

where $\binom{n}{i}$ means the number of choices of i elements from n.

PROOF. Assume that v and v' are vectors with weights at most equal to t and that they are in the same coset. It is clear that $v - v' \in C$ and so that $w(v-v') \geq 2t+1$. But, on the other hand, $w(v-v') \leq w(v') \leq 2t$, which is a contradiction.
□

Proposition 4. *For transmission over a binary symmetric channel, decoding using the standard array coincides with the minimum error probability decoding rule (maximum likelihood) if the coset-leader is a minimum weight vector in each coset.*

PROOF. Let p be the probability of error for the binary symmetric channel (cf Definition 9, Chapter 1). The probability of correct decoding for a transmitted codeword v is equal to the probability that the received vector v' is in the same column of v in the standard array. Let $P_C(v)$ be the probability of correct decoding of v, we can write:

$$\begin{aligned} P_C(v) &= \sum_{v' \in C(v)} p^{d(v,v')}(1-p)^{n-d(v,v')} \\ &= \sum_{u \in CL} p^{w(u)}(1-p)^{n-w(u)} \\ &= \sum_{u \in CL} (1-p)^n (p/(1-p))^{w(u)} \end{aligned}$$

where $C(v)$ is the set of vectors which are in the same column as v and CL is the set of coset-leaders in the standard array.

It is clear that $P_C(v)$ is maximum when the coset-leader has minimum weight. So, p is always less that 1/2 and to maximize $P_C(v)$ reduces to minimizing the error probability of decoding from the standard array.

□

4.2.6.2 Syndrome calculation

From the decoding rule in Section 4.2.6.1, it is necessary to look for the position of the received vector v' in the standard array to give the codeword in the same column. For linear codes with large parameters, this becomes a difficult problem to solve because of memory as well as time limitations. For example, if we use a binary code with parameters $n = 32$ and $k = 6$, it requires 16GBytes to store the 2^{26} cosets, with 2^6 vectors each of 32 bits. We can reduce this difficulty by using the code's parity-check matrix to define a syndrome function.

Definition 8. Let $C(n, k)$ be a linear code. A parity-check matrix allows us to define the linear function:

$$s\colon [GF(2)]^n \to [GF(2)]^{n-k}$$

$$v \to s(v) = vH^t$$

where $s(v)$ is called the *syndrome of vector* v, and s is called the *syndrome function*.

Remark 9. Two vectors have the same syndrome if and only if their difference is a codeword. All the vectors in the same coset $u + C$ have the same syndrome $s(u)$. (cf. Proposition 25, Chapter 2).

Lemma 3. *There exists a bijection between the set of 2^{n-k} cosets of a linear code $C(n, k)$, and the set of the 2^{n-k} possible images of s.*

Proof. Assume that $u_i + C$ and $u_j + C$ have the same syndrome. Then $s(u_i) = s(u_j)$:

$$0 = s(u_i) - s(u_j) = s(u_i - u_j)$$

which reduces to saying that $u_i - u_j \in C$ which contradicts Proposition 3 (cf. Proposition 25, Chapter 2).

□

4.2.6.3 Decoding by syndrome

The one-to-one correspondance between cosets and syndromes (Lemma 3) entails that we can redefine the decoding rule in Section 4.2.6.1 thus:

(1) Let v' be the received vector, compute its syndrome $s(v')$.
(2) Determine which is the coset-leader u_i with the same syndrome.
(3) Decode v' by $v' - u_i$.

This decoding rule coincides with the minimum distance decoding rule. It also coincides with the minimum error probability rule (i.e., the maximum likelihood rule) for transmission over a binary symmetric channel.

EXAMPLE 5. We again use the linear code whose generator and control matrices were given in Example 1, and we construct its standard array.

$\mathcal{C}$	000000	110110	011101	101011	100101	010011	111000	001110
$u_1 + \mathcal{C}$	100000	010110	111101	001011	000101	110011	011000	101110
$u_2 + \mathcal{C}$	010000	100110	001101	111011	110101	000011	101000	011110
$u_3 + \mathcal{C}$	001000	111110	010101	100011	100011	011011	110000	000110
$u_4 + \mathcal{C}$	000100	110010	011001	101111	101111	010111	111100	001010
$u_5 + \mathcal{C}$	000010	110100	011111	101001	101001	010001	111010	001100
$u_6 + \mathcal{C}$	000001	110111	011100	101010	101010	010010	111001	001111
$u_7 + \mathcal{C}$	001001	111111	010100	100010	100010	011010	110001	000111

Let us assume that, during transmission of a codeword (100101), there occurs an error, for example at the fifth coordinate. We will therefore receive the vector (100111). The decoder makes the following steps:

(1) Compute the syndrome:

$$s(100111) =$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}$$

(there is error detection, because the syndrome is not the zero vector).

(2) Determine that the coset-leader (000010) has the same syndrome (011).

(3) Decode (100111) by the codeword (100111) − (000010) = (100101). In this case, decoding was correct because the code is 1-corrector.

On the other hand, if we assume that there are two errors, for example in the second and fifth coordinate, we will then receive the vector (110111). The decoder will perform the following steps:

(1) Compute the syndrome:

$$s(110111) = (110111)\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (1 \quad 0 \quad 0)$$

(error detection because the syndrome is not the zero vector).

(2) Verify that the coset-leader (000001) has the same syndrome (100).

(3) Decode (110111) by the codeword (110111) − (000001) = (110110). In this case, decoding is incorrect because the code is 1-corrector and there are two errors in transmission.

REMARK 10. We note that we could have taken all the vectors of weight 1 as coset-leaders because the code is 1-corrector.

4.2.7 Weight enumerator polynomials and MacWilliams identities

The minimum distance of a linear code gives us the capacity for detection and correction for the code, if we use the minimum distance decoding rule. But we need to know more about distances or weights of the codewords, and of the vectors in their cosets to be able to calculate the transmission error probability. We use then the polynomial enumerator of the weights in the code, or in the cosets, respectively.

This polynomial is very useful in the study of combinatorial properties of codes, whether they be linear or not. This combinatorial point of view is developed in Chapter 7 on the basis of this section and the next. The reader can skip Sections 4.2.7 and 4.2.8 on the first reading if he is not interested in combinatorial aspects of codes.